EE4205

Quantum Communication and Cryptography

1 Linear algebra

1.1 Definitions

$|v\rangle$ ket $\Rightarrow$ column vector, i.e. $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$, $\langle v|$ bra $\Rightarrow$ row vector, i.e. $\begin{pmatrix} r_1 & r_2 \end{pmatrix}$

$\langle v|^\dagger = \langle v|^{*^T} = |v\rangle$, i.e. $\langle v|$ is the complex conjugate of $|v\rangle$

$$m \times n \text{ matrix } M = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}, \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$|+\rangle = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, |-\rangle = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \langle +| = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \end{pmatrix}, \langle -| = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \end{pmatrix}$$

$$|+_i\rangle = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, |-_i\rangle = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}, \langle +_i| = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \end{pmatrix}, \langle -_i| = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \end{pmatrix}$$

1.2 Arithmetic

Inner product $\langle v_1|v_2\rangle = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = ac + bd$, Outer product $|v_1\rangle\langle v_2| = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}$

$$|v_1\rangle \otimes |v_2\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c \\ d \end{pmatrix} \\ b \begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ bd \\ bc \\ bd \end{pmatrix} = |v_1 v_2\rangle$$

$$\langle v_1| \otimes \langle v_2| = \begin{pmatrix} a & b \end{pmatrix} \otimes \begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} a \begin{pmatrix} c & d \end{pmatrix} & b \begin{pmatrix} c & d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac & ad & bc & bd \end{pmatrix} = \langle v_1 v_2|$$

$$|v_1\rangle \otimes \langle v_2| = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix} = |v_1\rangle\langle v_2|$$

$$\langle v|M\rangle = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c & e \\ d & f \end{pmatrix} = \begin{pmatrix} ac + bd & ae + bf \end{pmatrix}, \langle M|v\rangle = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} ae + cf \\ be + df \end{pmatrix}$$

$$\langle M|N\rangle = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} e & g \\ f & h \end{pmatrix} = \begin{pmatrix} ae + cf & ag + ch \\ be + df & bg + dh \end{pmatrix}$$

$(A \cdot B) \otimes (C \cdot D) = (A \otimes C) \cdot (B \otimes D)$

$(A \pm B) \otimes C = A \otimes C \pm B \otimes C$, $A \otimes (B \pm C) = A \otimes B \pm A \otimes C$, $(A \otimes B) \otimes C = A \otimes (B \otimes C)$

1.3 Properties

1.3.1 Normality

A vector v is normalized if it has norm $= \sqrt{\langle v|v\rangle} = 1$.
To normalize v, multiply v with the inverse of its norm $\Rightarrow \frac{1}{\sqrt{\langle v|v\rangle}}v$.

Two vectors u and v are orthogonal if $\langle u|v\rangle = 0 = \langle v|u\rangle$.
Two vectors u and v are orthonormal if they are orthogonal, and also both normalized.
An orthonormal basis B is an orthonormal vector set $\{v_1, v_2, ..., v_m\}$ in vector space $V \in \mathbb{C}^n$ such that all vectors $\{u_1, u_2, ..., u_m\} \in V$ can be expressed as $u_1 = c_1v_1 + c_2v_2 + ... + c_mv_m$.
An example orthonormal basis is $\{\alpha|0\rangle + \beta|1\rangle, \beta|0\rangle - \alpha|1\rangle\}$, $\alpha, \beta \in \Re$.

1.3.2 Operators

The transpose of a matrix is an operator which flips a $m \times n$ matrix M over its diagonal, producing $n \times m$ matrix $M^T \Rightarrow M = (M^T)^T$.
The conjugate transpose of a matrix is an operator which transposes a $m \times n$ matrix M and applies complex conjugation to every entry, producing $n \times m$ matrix $M^\dagger \Rightarrow M = (M^\dagger)^\dagger$.

Example: $M = \begin{pmatrix} a & c & e \\ b & d & f \end{pmatrix}, M^T = \begin{pmatrix} a & b \\ c & d \\ e & f \end{pmatrix}, M^\dagger = \begin{pmatrix} a^* & b^* \\ c^* & d^* \\ e^* & f^* \end{pmatrix}$

A square matrix is a matrix with the same number of rows and columns.
A $n \times n$ square matrix M is invertible if there exists its multiplicative inverse $n \times n$ square matrix M^{-1} such that $MM^{-1} = M^{-1}M = \mathbb{I}_n$.

A $n \times n$ square matrix M is orthogonal if $M^T = M^{-1} \Rightarrow M^TM = MM^T = \mathbb{I}_n$.
A $n \times n$ square matrix M is unitary if $M^\dagger = M^{-1} \Rightarrow M^\dagger M = MM^\dagger = \mathbb{I}_n$.
A square matrix M is Hermitian if $M^\dagger = M$.

1.3.3 Eigenvalues & Eigenvectors

A scalar λ and non-zero vector v are called an eigenvalue and eigenvector pair of a matrix M if $Mv = \lambda v$.
A $n \times n$ square matrix will have n eigenvalue and eigenvector pairs.

$$M_{2\times2} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}, \; M_{3\times3} = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix}$$

The determinant of a matrix is also the product of its eigenvalues, i.e. $\det(M_{2\times2}) = ad - bc = \lambda_1\lambda_2$, $\det(M_{3\times3}) = a(ei - fh) - b(di - fg) + c(dh - eg) = \lambda_1\lambda_2\lambda_3$.
The trace of a matrix is the sum of its diagonal elements and also its eigenvalues, i.e. $\mathrm{tr}(M_2) = a + d = \lambda_1 + \lambda_2$, $\mathrm{tr}(M_3) = a + e + i = \lambda_1 + \lambda_2 + \lambda_3$. However, this does not imply that $a = \lambda_1$ and $d = \lambda_2$ or vice versa.

1.3.4 Pure qubit states

The pure quantum state of a qubit $|\phi\rangle_1$ can be represented by a linear superposition of its two orthonormal basis vectors, known as the computational basis $\{|0\rangle, |1\rangle\}$. Mathematically, this is represented as the state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. Individually, $p_0 = |\alpha|^2$ and $p_1 = |\beta|^2$, where p_b is the probability of the measurement bit $b \in \{0, 1\}$, or the probability of ϕ outputting b when measured.

It follows for 2-qubit systems that their pure quantum state is $|\phi\rangle_2 = \alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\delta|11\rangle$, again with $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Then, the probability of the measurement outcomes are given by $p_{|00\rangle} = \alpha^2$, $p_{|01\rangle} = \beta^2$, $p_{|10\rangle} = \gamma^2$, $p_{|11\rangle} = \delta^2$, which is the overlap of x with $|\phi\rangle\langle\phi|$: $p_x = |\langle x|\phi\rangle|^2 = \langle x|\phi\rangle\langle\phi|x\rangle$.

Generalizing, the pure quantum state of a n-qubit system is defined as $|\phi\rangle_n = \sum_{x\in\{0,1\}^n} \sqrt{p_x}|x\rangle$, with $\sqrt{p_x} \in \mathbb{C}$ and $\sum_x |\sqrt{p_x}|^2 = 1$.

1.3.5 Mixed qubit states

$$\rho_{AB} = \begin{pmatrix} a & e & i & m \\ b & f & j & n \\ c & g & k & o \\ d & h & l & p \end{pmatrix}$$

The subsystems of a 2-qubit density matrix ρ_{AB} are defined by the partial traces:

$$\mathrm{tr}_B(\rho_{AB}) = \rho_A = \begin{pmatrix} a+f & i+n \\ c+h & k+p \end{pmatrix}, \ \mathrm{tr}_A(\rho_{AB}) = \rho_B = \begin{pmatrix} a+k & e+o \\ b+l & f+p \end{pmatrix}$$

1.3.6 Entanglement

A classical state is always unentangled.

The pure quantum state of a n-qubit system is separable if and only if it can be expressed as $|\phi\rangle_n = \bigotimes_i^n |\phi_i\rangle$.

It suffices to check for separability of pure quantum states by comparing coefficients of their product state, i.e. if $|\phi\rangle_2 = \alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\delta|11\rangle$, then it is separable if and only if $|\phi\rangle_2 = (A|0\rangle+B|1\rangle)(C|0\rangle+D|1\rangle)$. This implies $|\phi\rangle_2 = AC|00\rangle + AD|01\rangle + BC|10\rangle + BD|11\rangle \Rightarrow \alpha \cdot \delta = \beta \cdot \gamma$ for separability.

A mixed 2-qubit system is separable if its density matrix can be expressed as $\rho_{AB} = \sum_x p_x \rho_{A|x} \otimes \rho_{B|x}$. It suffices to check for separability of mixed systems by transposing the subsystem on B and checking for positive semidefiniteness, i.e. ρ_{AB} is separable if and only if $(\mathrm{tr}_A(\rho_{AB}))^T = (\rho_B)^T = \begin{pmatrix} a+k & b+l \\ e+o & f+p \end{pmatrix}$ is Hermitian and has positive eigenvalues.

1.4 Useful identities

Maximally mixed states: $\frac{\mathbb{I}_n}{n}$, where $\mathbb{I}_n$ is the $n \times n$ identity matrix $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$

$\mathbb{I}_2 = |0\rangle\langle 0| + |1\rangle\langle 1| = |+\rangle\langle +| + |-\rangle\langle -| = |+_i\rangle\langle +_i| + |-_i\rangle\langle -_i| = \sigma_x^2 = \sigma_y^2 = \sigma_z^2$
$\mathbb{I}_4 = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11| = |++\rangle\langle ++| + |+-\rangle\langle +-| + |-+\rangle\langle -+| + |--\rangle\langle --|$

Quantum logic gates				
	H	σ_x	σ_y	σ_z
01	$\frac{1}{\sqrt{2}}(\|0\rangle\langle 0\| + \|0\rangle\langle 1\| + \|1\rangle\langle 0\| - \|1\rangle\langle 1\|)$	$\|0\rangle\langle 1\| + \|1\rangle\langle 0\|$	$i(\|1\rangle\langle 0\| - \|0\rangle\langle 1\|)$	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$
$+-$	$\|0\rangle\langle +\| + \|1\rangle\langle -\|$	$\|+\rangle\langle +\| - \|-\rangle\langle -\|$	$i(\|+\rangle\langle -\| - \|-\rangle\langle +\|)$	$\|+\rangle\langle -\| + \|-\rangle\langle +\|$
	$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
λ	$\lambda_1 = 1, \lambda_2 = -1$	$\lambda_1 = 1, \lambda_2 = -1$	$\lambda_1 = 1, \lambda_2 = -1$	$\lambda_1 = 1, \lambda_2 = -1$
E_λ	$E_{\lambda_1} = \begin{pmatrix} 1+\sqrt{2} \\ 1 \end{pmatrix}, E_{\lambda_2} = \begin{pmatrix} 1-\sqrt{2} \\ 1 \end{pmatrix}$	$E_{\lambda_1} = \|+\rangle, E_{\lambda_2} = \|-\rangle$	$E_{\lambda_1} = \|+_i\rangle, E_{\lambda_2} = \|-_i\rangle$	$E_{\lambda_1} = \|0\rangle, E_{\lambda_2} = \|1\rangle$

Precomputations				
	00	01	10	11
$\|xy\rangle$	$\|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$	$\|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$	$\|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$
$\langle xy\|$	$\langle 00\| = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$	$\langle 01\| = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}$	$\langle 10\| = \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix}$	$\langle 11\| = \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}$
$\|x\rangle\langle y\|$	$\|0\rangle\langle 0\| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	$\|0\rangle\langle 1\| = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$	$\|1\rangle\langle 0\| = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$	$\|1\rangle\langle 1\| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$
	$++$	$+-$	$-+$	$--$
$\|xy\rangle$	$\|++\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$	$\|+-\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$	$\|-+\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}$	$\|--\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}$
$\langle xy\|$	$\langle ++\| = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$	$\langle +-\| = \frac{1}{2}\begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}$	$\langle -+\| = \frac{1}{2}\begin{pmatrix} 1 & 1 & -1 & -1 \end{pmatrix}$	$\langle --\| = \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & 1 \end{pmatrix}$
$\|x\rangle\langle y\|$	$\|+\rangle\langle +\| = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	$\|+\rangle\langle -\| = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$	$\|-\rangle\langle +\| = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$	$\|-\rangle\langle -\| = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$
	$0+$	$0-$	$1+$	$1-$
$\|xy\rangle$	$\|0+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$	$\|0-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$	$\|1+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$	$\|1-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$
$\langle xy\|$	$\langle 0+\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \end{pmatrix}$	$\langle 0-\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 & 0 & 0 \end{pmatrix}$	$\langle 1+\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}$	$\langle 1-\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0 & 1 & -1 \end{pmatrix}$
$\|x\rangle\langle y\|$	$\|0\rangle\langle +\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$	$\|0\rangle\langle -\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}$	$\|1\rangle\langle +\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$	$\|1\rangle\langle -\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix}$
	$+0$	-0	$+1$	-1
$\|xy\rangle$	$\|+0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$	$\|-0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}$	$\|+1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$	$\|-1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}$
$\langle xy\|$	$\langle +0\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}$	$\langle -0\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & -1 & 0 \end{pmatrix}$	$\langle +1\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}$	$\langle -1\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 & -1 \end{pmatrix}$
$\|x\rangle\langle y\|$	$\|+\rangle\langle 0\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$	$\|-\rangle\langle 0\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$	$\|+\rangle\langle 1\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	$\|-\rangle\langle 1\| = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}$

Maximally entangled Bell states				
	Φ^+	Φ^-	Ψ^+	Ψ^-
01 $+-$	$\frac{1}{\sqrt{2}}(00+11)$ $\frac{1}{\sqrt{2}}(++--)$	$\frac{1}{\sqrt{2}}(00-11)$ $\frac{1}{\sqrt{2}}(+-+-)$	$\frac{1}{\sqrt{2}}(01+10)$ $\frac{1}{\sqrt{2}}(++--)$	$\frac{1}{\sqrt{2}}(01-10)$ $\frac{1}{\sqrt{2}}(-+-+)$
$\lvert x\rangle$	$\lvert\Phi^+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$	$\lvert\Phi^-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$	$\lvert\Psi^+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$	$\lvert\Psi^-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$
$\langle x\rvert$	$\langle\Phi^+\rvert = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&1\end{pmatrix}$	$\langle\Phi^-\rvert = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&-1\end{pmatrix}$	$\langle\Psi^+\rvert = \frac{1}{\sqrt{2}}\begin{pmatrix}0&1&1&0\end{pmatrix}$	$\langle\Psi^-\rvert = \frac{1}{\sqrt{2}}\begin{pmatrix}0&1&-1&0\end{pmatrix}$
ρ_{AB}	$\lvert\Phi^+\rangle\langle\Phi^+\rvert = \frac{1}{2}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix}$	$\lvert\Phi^-\rangle\langle\Phi^-\rvert = \frac{1}{2}\begin{pmatrix}1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1\end{pmatrix}$	$\lvert\Psi^+\rangle\langle\Psi^+\rvert = \frac{1}{2}\begin{pmatrix}0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0\end{pmatrix}$	$\lvert\Psi^-\rangle\langle\Psi^-\rvert = \frac{1}{2}\begin{pmatrix}0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0\end{pmatrix}$
ρ_A, ρ_B	$\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \frac{\mathbb{I}_2}{2}$	$\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \frac{\mathbb{I}_2}{2}$	$\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \frac{\mathbb{I}_2}{2}$	$\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \frac{\mathbb{I}_2}{2}$

Gate transformations				
	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert -\rangle$
H	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$
σ_x (bit)	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$-\lvert -\rangle$
σ_y (both)	$i\lvert 1\rangle$	$-i\lvert 0\rangle$	$-i\lvert -\rangle$	$i\lvert +\rangle$
σ_z (phase)	$\lvert 0\rangle$	$-\lvert 1\rangle$	$\lvert -\rangle$	$\lvert +\rangle$

Gate transformations				
	$\lvert\Phi^+\rangle$	$\lvert\Phi^-\rangle$	$\lvert\Psi^+\rangle$	$\lvert\Psi^-\rangle$
$(\sigma_x)_A \otimes \mathbb{I}_B$	$\lvert\Psi^+\rangle$	$-\lvert\Psi^-\rangle$	$\lvert\Phi^+\rangle$	$-\lvert\Phi^-\rangle$
$\mathbb{I}_A \otimes (\sigma_x)_B$	$\lvert\Psi^+\rangle$	$\lvert\Psi^-\rangle$	$\lvert\Phi^+\rangle$	$\lvert\Phi^-\rangle$
$(\sigma_z)_A \otimes \mathbb{I}_B$	$\lvert\Phi^-\rangle$	$\lvert\Phi^+\rangle$	$\lvert\Psi^-\rangle$	$\lvert\Psi^+\rangle$
$\mathbb{I}_A \otimes (\sigma_z)_B$	$\lvert\Phi^-\rangle$	$\lvert\Phi^+\rangle$	$-\lvert\Psi^-\rangle$	$-\lvert\Psi^+\rangle$
$(\sigma_x\sigma_z)_A \otimes \mathbb{I}_B$	$-\lvert\Psi^-\rangle$	$\lvert\Psi^+\rangle$	$-\lvert\Phi^-\rangle$	$\lvert\Phi^+\rangle$
$\mathbb{I}_A \otimes (\sigma_x\sigma_z)_B$	$\lvert\Psi^-\rangle$	$\lvert\Psi^+\rangle$	$-\lvert\Phi^-\rangle$	$-\lvert\Phi^+\rangle$
$(\sigma_z\sigma_x)_A \otimes \mathbb{I}_B$	$\lvert\Psi^-\rangle$	$-\lvert\Psi^+\rangle$	$\lvert\Phi^-\rangle$	$-\lvert\Phi^+\rangle$
$\mathbb{I}_A \otimes (\sigma_z\sigma_x)_B$	$-\lvert\Psi^-\rangle$	$-\lvert\Psi^+\rangle$	$\lvert\Phi^-\rangle$	$\lvert\Phi^+\rangle$

Tripartite states		
	GHZ_3	W_3
01 $+-$	$\frac{1}{\sqrt{2}}(000+111)$ $\frac{1}{\sqrt{2}}(+++++---+-+-+--+)$	$\frac{1}{\sqrt{3}}(001+010+100)$
$\mathrm{tr}_E(\rho_{ABE})$ $\mathrm{tr}_{AB}(\rho_{ABE})$	$\rho_{AB} = \frac{1}{2}(\lvert 00\rangle\langle 00\rvert + \lvert 11\rangle\langle 11\rvert)_{AB}$ $\rho_E = \frac{\mathbb{I}_E}{2}$	$\rho_{AB} = \frac{1}{3}(\lvert 00\rangle\langle 00\rvert + \lvert 01\rangle\langle 01\rvert + \lvert 01\rangle\langle 10\rvert + \lvert 10\rangle\langle 01\rvert + \lvert 10\rangle\langle 10\rvert)_{AB}$ $\rho_E = \frac{1}{3}(2\lvert 0\rangle\langle 0\rvert + \lvert 1\rangle\langle 1\rvert)_E$
Theory	Both subsystems are classical and are unentangled.	ρ_{AB} is entangled while ρ_E is not.

2 Measurements

2.1 Density matrices

A density matrix ρ describes the probability distribution over the quantum states of a physical system. Unlike pure qubit systems, the described physical system could consist of non-independent qubit states. Density matrices able to describe these mixed qubit states.

A density matrix must fulfill the following:

1. Positive semi-definite, i.e. Hermitian and positive eigenvalues
2. Unit trace, i.e. $\text{tr}(\rho) = 1$

If a device prepares state $|\psi_x\rangle$ with probability p_x, the density matrix describing the state is defined as $\rho = \sum_x p_x |\psi_x\rangle\langle\psi_x|$.

A density matrix describes a pure state if and only if:

1. It can be written as an outer product of a state vector $|\psi\rangle$ with itself, i.e. $\rho = |\psi\rangle\langle\psi|$
2. It is a projection, i.e. its eigenvalues must be either 0 or 1.
   (a) By extension of being a projection, it is idempotent and has purity one, i.e. $\rho = \rho^2,\ \text{tr}(\rho) = \text{tr}(\rho^2) = 1$

A density matrix describes a classical state if and only if it is a diagonal matrix $\rho = \sum_x p_x |x\rangle\langle x|$. The only pure and classical states are $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$.

A density matrix describes a classical-quantum state (i.e. a partially classical and partially quantum state) if it has the form $\rho_{CQ} = \sum_x p_x |x\rangle\langle|x_C \otimes \rho_x^Q$, where C is the classical subsystem and Q is the quantum subsystem.

2.2 POVMs

Measurements performed upon a density matrix are made using a chosen orthonormal basis. These measurements can be described mathematically as positive operator-valued measures, or POVMs. A POVM on $\mathbb{C}^n$ is a set of positive semidefinite matrices $\{M_x\}_{x \in X}$ such that $\sum_x M_x = \mathbb{I}_n$.

A density matrix ρ allows for the calculation of the probabilities of any outcomes of any POVM M_x performed upon this system, using the Born rule: $p_x = \text{tr}(\rho M_x)$. Due to the cyclicity of the trace operator, if the system is a pure state, $p_x = \text{tr}(|\psi\rangle\langle\psi|M_x) = \text{tr}(\langle\psi|M_x|\psi\rangle) = \langle\psi|M_x|\psi\rangle$ as the trace of a scalar (in this case, an inner product) is simply the scalar itself.

Let Alice and Bob share a state ρ_{AB} (by using a photon laser and polarizing beam splitters to describe horizontal and vertical photon polarization as 0 and 1, or using down-conversion crystals to release two photons that have half the energy of a single photon input and opposite polarization for entanglement, etc.). After Alice performs a measurement (i.e. measuring the polarization of the photon input), she obtains a classical output bit x (corresponding to the polarization of the measured photon) and Bob's resulting post-measurement state (since the photon is consumed) is given by $\rho_{B|x} = \frac{\sqrt{M_x} \otimes \mathbb{I}_B \rho_{AB} \sqrt{M_x} \otimes \mathbb{I}_B}{\text{tr}[\rho_{AB} \sqrt{M_x} \otimes \mathbb{I}_B]}$. Bob is effectively idle during Alice's independent measurement process, hence M_x is tied to $\mathbb{I}_B$, and the resulting system conditioned on the outcome x is normalized over the probability of that outcome.

Example 1: Alice and Bob share $\rho_{AB} = |\Phi^+\rangle\langle\Phi^+|$. Alice measures in the computational basis $\{|0\rangle, |1\rangle\}$. The probability of the outcomes are then given by the Born rule using the observable on the composite system $M_{x,A} \otimes \mathbb{I}_B$: $p_0 = \text{tr}(\rho_{AB}(|0\rangle\langle 0| \otimes \mathbb{I}_B)) = \frac{1}{2}$ and $p_1 = \text{tr}(\rho_{AB}(|1\rangle\langle 1| \otimes \mathbb{I}_B)) = \frac{1}{2}$. The resulting post-measurement states for each observable are then given by: $\rho_{B|0} = \frac{(|0\rangle\langle 0|\otimes \mathbb{I}_B)\rho_{AB}(|0\rangle\langle 0|\otimes \mathbb{I}_B)}{p_0} = \frac{\frac{1}{2}|00\rangle\langle 00|}{\frac{1}{2}}$ and $\rho_{B|1} = \frac{(|1\rangle\langle 1|\otimes \mathbb{I}_B)\rho_{AB}(|1\rangle\langle 1|\otimes \mathbb{I}_B)}{p_1} = \frac{\frac{1}{2}|11\rangle\langle 11|}{\frac{1}{2}}$. It can then be seen that Bob will always obtain the same outcome x as Alice if he also performs a measurement in the computational basis on $\rho_{B|x}$.

Example 2: Alice and Bob share $\rho_{AB} = \frac{1}{2}(|0\rangle\langle 0|_A \otimes |1\rangle\langle 1|_B + |+\rangle\langle +|_A \otimes |-\rangle\langle -|_B)$. A simultaneous measurement is performed on both qubits in the computational basis $\{|0\rangle, |1\rangle\}$. The probability of the outcomes are then:

1. $p_{A=|0\rangle, B=|0\rangle} = \frac{1}{2}(1 \cdot 0 + \frac{1}{2} \cdot \frac{1}{2}) = \frac{1}{8}$
2. $p_{A=|0\rangle, B=|1\rangle} = \frac{1}{2}(1 \cdot 1 + \frac{1}{2} \cdot \frac{1}{2}) = \frac{5}{8}$
3. $p_{A=|1\rangle, B=|0\rangle} = \frac{1}{2}(0 \cdot 0 + \frac{1}{2} \cdot \frac{1}{2}) = \frac{1}{8}$
4. $p_{A=|1\rangle, B=|1\rangle} = \frac{1}{2}(0 \cdot 1 + \frac{1}{2} \cdot \frac{1}{2}) = \frac{1}{8}$

2.3 Uncertainty & randomness extraction

The probability of guessing is always taken to be the best guess out of all the guesses $p_{\text{guess}}(X) = \max_x p_x$. The minimum entropy represents the uncertainty of the outcome, defined by $H_{\min}(X) = -\log(p_{\text{guess}}(X))$. These two share an inverse relationship: the higher the probability of guessing, the lower the minimum entropy and therefore lower uncertainty.

The conditional minimum entropy $H_{\min}(X|Q)$ of a classical-quantum state $\rho_{CQ} = \sum_x p_x |x\rangle\langle|x_C \otimes \rho_x^Q$ is defined through the conditional guessing probability $p_{\text{guess}}(X|Q) = \max_{\{M_x\}_x} \sum_x p_x \text{tr}(M_x \rho_x^Q)$.

For any POVM $\{M_x\}$ and any quantum state ρ_x^Q, we have $\text{tr}(M_x\rho_x^Q) \leq \lambda_{\max}(\rho_x^Q)\text{tr}(M_x) \leq \text{tr}(M_x)$. Then, $\sum_x p_x \text{tr}(M_x\rho_x^Q) \leq \sum_x p_x \text{tr}(M_x) \leq \max_x p_x \sum_x \text{tr}(M_x) = \max_x p_x \text{tr}(\sum_x M_x) = \max_x p_x \text{tr}(\mathbb{I}_Q) = \max_x p_x |Q|$.

Therefore, $p_{\text{guess}}(X|Q) = \max_{\{M_x\}_x} \sum_x p_x \text{tr}(M_x\rho_x^Q) \leq \max_x p_x |Q|$.

$\Rightarrow H_{\min}(X|Q) = -\log(p_{\text{guess}}(X|Q)) \geq -\log(\max_x p_x |Q|) = -\log(\max_x p_x) - \log|Q| = H_{\min}(X) - \log|Q|$.

The conditional minimum entropy $H_{\min}(X|Q)$ of a classical-quantum state ρ_{CQ} only fulfills the chain rule if X and Q are independent systems $\Rightarrow H_{\min}(QX) = -\log(p_{\text{guess}}(QX)) = -\log(p_{\text{guess}}(Q)p_{\text{guess}}(X))$
$= -\log(p_{\text{guess}}(Q)) - \log(p_{\text{guess}}(X)) = H_{\min}(Q) + H_{\min}(X)$ and from $H_{\min}(X|Q) = H_{\min}(X)$, we have $H_{\min}(X|Q) = H_{\min}(QX) - H_{\min}(Q)$. If X and Q are not independent, there is no certain form of the chain rule for conditional minimum entropy.

2.4 Quantum channels

A quantum channel is a map that transmits quantum information in the form of qubits between two parties. For any $n, m \geq 0$, a quantum channel from n qubits to m qubits is any function $\mathcal{N}$ from $(\mathbb{C}^2)^{\otimes n}$ to $(\mathbb{C}^2)^{\otimes m}$ that can be expressed as a sequence of extra qubit preparation, unitary operation and tracing out.

Quantum depolarizing channels are often used for state sharing. They are completely-positive trace preserving (CPTP) maps that model external noise affecting the n-qubit quantum transmission, given by $\mathcal{N}_\epsilon(\rho) = (1-\epsilon)\rho + \frac{\epsilon\mathbb{I}}{2^n}\text{tr}(\rho)$, $\epsilon \in [0, 1]$.

Suppose Alice shares Φ^+ with Bob by sending one of the two qubits in the system to Bob through the channel. Due to the channel, the depolarized state ρ_B that Bob receives is then given by $\rho_B = (1-\epsilon)\text{tr}_A(|\Phi^+\rangle\langle\Phi^+|) + \frac{\epsilon\mathbb{I}}{2}\text{tr}(\text{tr}_A(|\Phi^+\rangle\langle\Phi^+|)) = (1-\epsilon)\frac{\mathbb{I}}{2} + \frac{\epsilon\mathbb{I}}{2}\text{tr}(\frac{\mathbb{I}}{2}) = \frac{\mathbb{I}}{2} = \text{tr}_A(|\Phi^+\rangle\langle\Phi^+|)$, which is what Bob expects to receive as his subsystem of Φ^+.

3 One-time pad

3.1 Classical

Recall the classical one-time pad to be the following encryption and decryption scheme:

$$c = m \oplus k$$

$$m = c \oplus k$$

where c is the ciphertext, m is the plaintext and k is a uniformly random generated secret key. The following truth table is obtained for each bit under observation:

m	k	c
0	0	0
0	1	1
1	0	1
1	1	0

The one-time pad is correct due to the reversibility of the encryption:
$(m \oplus k) \oplus k = c \oplus k = m$ and $(c \oplus k) \oplus k = m \oplus k = c$.

The probability of guessing the ciphertext given the n-bit length plaintext is given by
$\Pr(C = c|M = m) = \Pr(K \oplus M = c|M = m) = \Pr(K \oplus m = c) = \Pr(K = m \oplus c) = \Pr(K = k) = (\frac{1}{2})^n$.

The probability of guessing the plaintext given the ciphertext is then given by
$\Pr(M = m|C = c) = \frac{\Pr(C=c|M=m)\cdot\Pr(M=m)}{\Pr(C=c)} = \frac{\Pr(K=k)\cdot\Pr(M=m)}{\Pr(K=k)} = \Pr(M = m)$.

This is because the secret key is uniformly random generated, and without knowledge of the key, the ciphertext gives no information about the plaintext, and vice-versa. This proves the perfect secrecy of the one-time pad.

3.2 Quantum

The quantum one-time pad now deals with qubits that can take the states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Observe that to mimic the bitwise XOR operation, the Pauli X and Z gates need to be applied depending on the state of the qubits. We then arrive at the following encryption and decryption scheme:

$$|c\rangle = \sigma_x^{k_1}\sigma_z^{k_2}|m\rangle$$

$$|m\rangle = \sigma_z^{k_2}\sigma_x^{k_1}|c\rangle$$

where $|c\rangle$ is a ciphertext qubit, $|m\rangle$ is a plaintext qubit and $(k_1, k_2) \in \{0, 1\}$.

Eve will only see the maximally mixed state averaged out across the four permutations of (k_1, k_2), given by: $\frac{1}{4}\sum_{k_1,k_2\in\{0,1\}} \sigma_x^{k_1}\sigma_z^{k_2}|m\rangle\langle m|\sigma_z^{k_2}\sigma_x^{k_1} = \frac{\mathbb{I}}{2}$, and she cannot gain any information about $|m\rangle\langle m|$.

4 Quantum money

A quantum money scheme is a protocol that creates and verifies quantum banknotes that are resistant to forgery due to using quantum states that cannot be copied as per the no-cloning theorem. Practically, this is not feasible due to the short lifetime of quantum memory as a result of decoherence.

4.1 No-cloning theorem

Suppose there is a unitary operator C such that for all normalized states $|\phi\rangle_A$ and $|\psi\rangle_B$: $C(|\phi\psi\rangle_{AB}) = |\phi\phi\rangle_{AB}$. C is cloning the arbitrary qubit $|\phi\rangle_A$.

Since C is unitary, $C^\dagger C = \mathbb{1}$. Then,

$$\langle\phi_1|\phi_2\rangle = \langle\phi_1|\phi_2\rangle\langle\psi|\psi\rangle$$

$$= \langle\phi_1\psi|\phi_2\psi\rangle = \langle\phi_1\psi|C^\dagger C|\phi_2\psi\rangle$$

$$= \langle\phi_1\phi_1|\phi_2\phi_2\rangle = (\langle\phi_1|\phi_2\rangle)^2$$

This implies that $|\langle\phi_1|\phi_2\rangle| = 0, 1$, or ϕ_1 is orthogonal to ϕ_2. This is not necessarily the case for arbitrary states ϕ_1 or ϕ_2. Therefore, there does not exist a universal C that can clone a general quantum state.

Since quantum states cannot be perfectly duplicated, it is impossible to forge quantum money by including quantum systems in its design.

4.2 Wiesner's scheme

The bank needs to perform two procedures:

1. Produce quantum bills. Similar to classical bank notes, a serial number \$ is selected arbitrarily. Then, two bitstrings $x, \theta \in \{0,1\}^n$ are uniformly random generated. The bank stores these strings as a private key $k = (x, \theta)$ and creates the quantum state $|\psi\rangle_\$ = \bigotimes_{i=1}^{n} H^{\theta_i}|x_i\rangle$.

2. Verify the legitimacy of quantum bills. The bank receives $|\psi\rangle_\$$ as defined in the production procedure. As $\bigotimes_{i=1}^{n} H^{\theta_i} \bigotimes_{i=1}^{n} H^{\theta_i} = 1$, the bank will measure $\bigotimes_{i=1}^{n} H^{\theta_i}|\psi\rangle_\$ = |x\rangle_\$$ in the computational basis to produce outcome $\hat{x}$. If $\hat{x} = x$, the quantum bill is accepted.

Effectively, the quantum bills contain a series of isolated two-state quantum systems represented by $|\psi\rangle_\$$. The key $k = (x, \theta)$ is used to obtain all the polarizations of these systems. The quantum bills only have the serial number \$ public while the key is kept private by the bank.

4.2.1 Security

Consider the single qubit version of Wiesner's scheme, i.e. $x, \theta \in \{0, 1\}$. Then, $|\psi\rangle_\$ = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The counterfeiter Charlie does not know which state $|\psi\rangle_\$$ is, and has to return a two-qubit system ρ that maximizes the verification success rate. Overall, the success probability that Charlie has against the scheme is then the average of the four possible outcomes $p_{\text{success}} = \frac{1}{4} \sum_{i\in\{0,1,+,-\}} \langle ii|\rho_i|ii\rangle$.

Charlie has two main attacks against Wiesner's scheme:

1. Measure and prepare: To compute $p_{\text{success}} = \frac{1}{4} \sum_{i \in \{0,1,+,-\}} \langle ii|\rho_i|ii\rangle = \frac{1}{4}(\langle 00|\rho_0|00\rangle + \langle 11|\rho_1|11\rangle + \langle ++|\rho_+|++\rangle + \langle --|\rho_-|--\rangle)$, Charlie must first produce a quantum channel that maps his measurement observable $|x\rangle\langle x|$ to the two-qubit system ρ_x that he will use. To measure $|\psi\rangle_\$$, Charlie decides on an arbitrary orthonormal basis $\{b_0, b_1\} = \{\alpha|0\rangle + \beta|1\rangle, \beta|0\rangle - \alpha|1\rangle\}$ for the single qubit space $\mathbb{C}^2$. Charlie returns the density matrix $\rho = |b_{xx}\rangle\langle b_{xx}|$ depending on the measurement outcome $x \in \{0,1\}$. Then, we have the map $|x\rangle\langle x| \mapsto \rho_x \coloneqq \sum_{X \in \{0,1\}} |b_{XX}\rangle\langle b_{XX}| p_{x|b_X}$, where the probability of the measurement outcome x when measuring using the basis state b_X is given by $p_{x|b_X} = \text{tr}(|x\rangle\langle x|b_X\rangle\langle b_X|) = |\langle b_X|x\rangle|^2$. He can then compute the following:

   (a) $\langle 00|\rho_0|00\rangle = \langle 00|b_{00}\rangle\langle b_{00}| \cdot |\langle b_0|0\rangle|^2 + |b_{11}\rangle\langle b_{11}| \cdot |\langle b_1|0\rangle|^2|00\rangle = |\alpha|^6 + |\beta|^6$

   (b) $\langle 11|\rho_1|11\rangle = \langle 11|b_{00}\rangle\langle b_{00}| \cdot |\langle b_0|1\rangle|^2 + |b_{11}\rangle\langle b_{11}| \cdot |\langle b_1|1\rangle|^2|11\rangle = |\beta|^6 + |\alpha|^6$

   (c) $\langle ++|\rho_+|++\rangle = \langle ++|b_{00}\rangle\langle b_{00}| \cdot |\langle b_0|+\rangle|^2 + |b_{11}\rangle\langle b_{11}| \cdot |\langle b_1|+\rangle|^2|++\rangle = \frac{|\alpha+\beta|^6}{8} + \frac{|\alpha-\beta|^6}{8}$

   (d) $\langle --|\rho_-|--\rangle = \langle --|b_{00}\rangle\langle b_{00}| \cdot |\langle b_0|-\rangle|^2 + |b_{11}\rangle\langle b_{11}| \cdot |\langle b_1|-\rangle|^2|--\rangle = \frac{|\alpha+\beta|^6}{8} + \frac{|\alpha-\beta|^6}{8}$

   Finally, $p_{\text{success}} = \frac{|\alpha|^6}{2} + \frac{|\alpha+\beta|^6}{16} + \frac{|\alpha-\beta|^6}{16} + \frac{|\beta|^6}{2} = \frac{5}{8}(\alpha^2+\beta^2)^3$. Given that $|\alpha|^2+|\beta|^2 = 1$, the probability of success is maximized at $\frac{5}{8}$, with one of the solutions being $\alpha = 0, \beta = 1 \Rightarrow \{b_0, b_1\} = \{|1\rangle, |0\rangle\}$.

2. Cloning: Charlie attempts to clone $|\psi\rangle_\$$ using a CPTP map $T(|\psi\rangle\langle\psi|) = A_1|\psi\rangle\langle\psi|A_1^\dagger + A_2|\psi\rangle\langle\psi|A_2^\dagger$, where (A_1, A_2) are valid Kraus operators. The operators must fulfill $A_1^\dagger A_1 + A_2^\dagger A_2 = \mathbb{I}$. The probability of success is then given by $p_{\text{success}} = \langle\psi|\langle\psi|T(|\psi\rangle\langle\psi|)|\psi\rangle|\psi\rangle$. This is maximized for the Kraus operators $(\frac{1}{\sqrt{12}} \begin{pmatrix} 3 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}, \frac{1}{\sqrt{12}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 3 \end{pmatrix})$ with a probability of $\frac{3}{4}$.

5 Quantum information & communication

5.1 Quantum secret sharing

Suppose there exists a private key k. k needs to be partitioned amongst several parties such that its partitions $k_1, k_2, ..., k_n$ are ambiguous individually, yet the union of these partitions allows for the recovering of k.

A trivial classical secret sharing scheme amongst two parties, Alice and Bob, would be to use the one-time pad. Uniformly random generate a plaintext m, then give Alice m and Bob the ciphertext $m \oplus k = c$. In this case, neither the plaintext nor the ciphertext reveal any information about the key on their own, so Alice and Bob are ignorant about k, but together they can recover k.

In similar fashion, the same can be performed using the maximally entangled states. Given that the subsystems of each of the Bell states are simply the maximally mixed state $\frac{\mathbb{I}}{2}$, if Alice and Bob are each given one of the two qubits from a Bell state, they cannot locally distinguish from their own system A or B which of the four Bell states was used.

Extending this to three parties, Alice, Bob and Charlie, the tripartite GHZ_3 state can be used in place of the Bell states, as the individual subsystems are also the maximally mixed states $\frac{\mathbb{I}}{2}$, and the paired subsystems are $\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ which is classical.

5.2 Quantum teleportation

The no-cloning theorem forbids the copying of arbitrary quantum states. As such, Alice needs a method to send Bob her quantum state. In fact, Alice can prepare her own state ρ_A on Bob's side without sending him any quantum information at all, using only two classical bits and a classical channel.

However, it isn't as simple as measuring her qubit in some chosen basis, preparing another qubit in the state she obtains and sending that to Bob. Recall that any measurement made on a quantum system disturbs it, so upon Alice measuring ρ_A, it will collapse to some eigenstate of the chosen basis, so if she reproduces the state and sends it to Bob, it will not be ρ_A but rather the post-measurement state of ρ_A.

Instead, what Alice could do is the following quantum teleportation scheme:

1. Alice holds the teleportable state $|\psi\rangle_T = \alpha|0\rangle + \beta|1\rangle$ and shares $|\Phi^+\rangle_{AB}$ with Bob. The joint state of all three qubits is then given by $|\theta\rangle_{TAB} = |\psi\rangle_T \otimes |\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle)_{TAB}$.

2. Observe that the joint state can be written as $|\theta\rangle_{TAB} = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle)_{TAB}$
   $= \frac{1}{2}(\alpha(|\Phi^+\rangle + |\Phi^-\rangle)|0\rangle + \beta(|\Psi^+\rangle - |\Psi^-\rangle)|0\rangle + \alpha(|\Psi^+\rangle + |\Psi^-\rangle)|1\rangle + \beta(|\Phi^+\rangle - |\Phi^-\rangle)|1\rangle)$
   $= \frac{1}{2}(|\Phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + |\Phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) + |\Psi^+\rangle(\beta|0\rangle + \alpha|1\rangle) + |\Psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle))$.

3. If Alice measures in the Bell basis, Bob's qubit is then $\{\alpha|0\rangle + \beta|1\rangle, \alpha|0\rangle - \beta|1\rangle, \beta|0\rangle + \alpha|1\rangle, -\beta|0\rangle + \alpha|1\rangle\}$ respectively. Alice sends this measurement outcome which is encoded using two classical bits.

4. To turn his qubit into $|\psi\rangle_T = \alpha|0\rangle + \beta|1\rangle$, Bob needs to apply the respective unitary transformations $\{\mathbb{I}, \sigma_z, \sigma_x, \sigma_{zx}\}$ depending on Alice's measurement outcome.

This should not be interpreted as converting Alice's arbitrary quantum state into a sequence of classical bits which Bob then uses to reconstruct Alice's original state, as this violates the no-cloning theorem: if it were possible to convert a qubit into classical bits, then a qubit would be easy to copy (since classical bits are trivially copyable). Rather, Alice's quantum state is first destroyed, and an exact replica is created by Bob.

5.3 Superdense coding

Instead of a classical channel, suppose Alice now only has a quantum channel that she can use to share two classical bits with Bob using a single qubit.

Alice's first idea was to encode her uniformly random generated two classical bits into her preparation of one of the four states $\in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and then send this qubit to Bob. Bob creates a POVM with four operators $\{M_0, M_1, M_+, M_-\}$ such that $p_{\text{guess}} = \frac{1}{4} \sum_{x \in \{0,1,+,-\}} \langle x|M_x|x\rangle$ is maximized.
Unfortunately, Bob's best guess is still only $p_{\text{guess}} = \frac{1}{2}$ when $\{M_0, M_1, M_+, M_-\} = \{|0\rangle\langle 0|, |1\rangle\langle 1|, 0, 0\}$. A different scheme is needed to achieve the communication with certainty:

1. Alice shares $|\Phi^+\rangle_{AB}$ with Bob.
2. Depending on her uniformly random generated two classical bits $(b_1, b_2) \in \{0, 1\}$, Alice applies one of the four unitary transformations $\{\mathbb{I}, \sigma_z, \sigma_x, \sigma_{zx}\}$ to her qubit and sends it to Bob.
3. Bob now has the qubit pair state $\frac{1}{\sqrt{2}}((\sigma_z^{b_1}\sigma_x^{b_2}|0\rangle_A) \otimes |0\rangle_B + (\sigma_z^{b_1}\sigma_x^{b_2}|1\rangle_A) \otimes |1\rangle_B)$. The possible values for this state are simply the four Bell states.
4. Bob measures his state in the Bell basis, and depending on the outcome $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$, he can discern b_1 and b_2.

Furthermore, observe that if Eve intercepts the qubit sent from Alice to Bob, she cannot recover information about b_1 or b_2. The subsystem sent by Alice after applying the unitary transformation is of the form $\frac{1}{2}(U|0\rangle\langle 0|U^\dagger + U|1\rangle\langle 1|U^\dagger) = U\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)U^\dagger = U\frac{\mathbb{I}}{2}U^\dagger = \frac{\mathbb{I}}{2}$. Eve only sees the maximally mixed state.

6 Quantum games

6.1 Bipartite guessing game

Suppose two parties, Alice and Eve, play the following game:

1. Eve prepares a qubit in an arbitrary state ρ_A and sends it to Alice.
2. Alice chooses a random bit $b \in \{0, 1\}$.
3. Alice measures ρ_A in the basis $b == 0\ ?\ \{|0\rangle, |1\rangle\} : \{|+\rangle, |-\rangle\}$.
4. Alice obtains a measurement outcome $x \in \{0, 1\}$ and announces b.
5. Eve wins if she can guess x.

Eve's guessing probability is given by $p_{\text{guess}}(x|b) = \frac{1}{2}(p_{\text{guess}}(x|b = 0) + p_{\text{guess}}(x|b = 0))$. Observe that Eve's only influence on her success is the state ρ_A that she prepares for Alice. As such, she has to maximize $p_{\text{guess}}(x|b)$ over ρ_A (without loss of generality, assume $x = 0$): $p_{\text{guess}}(x|b) = \frac{1}{2}(\text{tr}(\rho_A|0\rangle\langle 0|) + \text{tr}(\rho_A|+\rangle\langle +|)) = \frac{1}{2}\text{tr}(\rho_A(|0\rangle\langle 0| + |+\rangle\langle +|))$.

The expression is maximized when ρ_A is prepared in the pure state corresponding to the eigenvector v of $|0\rangle\langle 0| + |+\rangle\langle +|$ with the largest eigenvalue $\lambda_{\max} = 1 + \frac{1}{\sqrt{2}}$: $p_{\text{guess}}(x|b) = \frac{1}{2}\text{tr}(\rho_A(|0\rangle\langle 0| + |+\rangle\langle +|)) = \frac{\lambda_{\max}}{2}$. Then, it follows that $\text{tr}(\rho_A(|0\rangle\langle 0| + |+\rangle\langle +|)) = \lambda_{\max} \Rightarrow \rho_A = \lambda_{\max} \begin{pmatrix} \alpha^2 & \alpha\beta \\ \alpha\beta & \beta^2 \end{pmatrix}$, $\text{tr}(\begin{pmatrix} \alpha^2 & \alpha\beta \\ \alpha\beta & \beta^2 \end{pmatrix} \begin{pmatrix} \frac{3}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}) = 1$. Computing, we have $\rho_A = (1 + \frac{1}{\sqrt{2}}) \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = (2 + \sqrt{2})|-\rangle\langle -|$ and $p_{\text{guess}}(x|b) = \frac{1}{2} + \frac{1}{2\sqrt{2}}$.

Furthermore, if Eve is allowed to produce an arbitrary state ρ_{AE} and sends only the subsystem ρ_A to Alice, she can always guess perfectly if ρ_{AE} is maximally entangled. This produces two major conclusions:

1. Uncertainty principle: If Eve has minimal entanglement with Alice, then she cannot predict the outcomes of two incompatible measurements well. In particular, this means it is difficult for her to guess Alice's outcomes. There does not exist a single-qubit state that provides a deterministic outcome in both the computational and Hadamard bases.
2. Monogamy of entanglement: If Eve has maximal entanglement with Alice, she will always guess perfectly. Therefore, is necessary for Alice to maintain entanglement with another party, Bob, so that Eve has minimal entanglement with either Alice and Bob.

Suppose Alice wants to reduce the maximal entanglement she shares with Eve over the state Φ^+. She applies a unitary transformation to her qubit after generating b but before measuring. Their joint state is now given by $|\Phi^+\rangle_U = (U_A \otimes \mathbb{I}_E)|\Phi^+\rangle$. Of course, if Eve knows U_A, then she can reverse the unitary operation by applying the complex conjugate U_A^*. Otherwise, the outcomes are:

1. If $U \in \{\mathbb{I}, \sigma_z, \sigma_x, \sigma_{zx}\}$, Alice can do the following:

   (a) If $b = 0$, $U \coloneqq \begin{cases} \mathbb{I} & \text{with } p = \frac{1}{2} \Rightarrow |\Phi^+\rangle_U = |\Phi^+\rangle \\ \sigma_x & \text{with } p = \frac{1}{2} \Rightarrow |\Phi^+\rangle_U = |\Psi^+\rangle \end{cases}$

   (b) If $b = 1$, $U \coloneqq \begin{cases} \mathbb{I} & \text{with } p = \frac{1}{2} \Rightarrow |\Phi^+\rangle_U = |\Phi^+\rangle \\ \sigma_z & \text{with } p = \frac{1}{2} \Rightarrow |\Phi^+\rangle_U = |\Phi^-\rangle \end{cases}$

   Given that Eve will see the same subsystem in all cases, which is the maximally mixed state $\frac{\mathbb{I}}{2}$, she cannot distinguish between the two outcomes, so $p_{\text{guess}}(x|b) = \frac{1}{2}$.

2. If $U \in \{\mathbb{I}, \sigma_{xz}\}$, $U := \begin{cases} \mathbb{I} & \text{with } p = \frac{1}{2} \Rightarrow |\Phi^+\rangle_U = |\Phi^+\rangle \\ \sigma_{xz} & \text{with } p = \frac{1}{2} \Rightarrow |\Phi^+\rangle_U = -|\Psi^-\rangle \end{cases}$

   Given that Eve will see the same subsystem in all cases, which is the maximally mixed state $\frac{\mathbb{I}}{2}$, she cannot distinguish between the two outcomes, so $p_{\text{guess}}(x|b) = \frac{1}{2}$.

6.2 CHSH game

6.2.1 Classical

Suppose three parties, Alice, Bob and Charlie, play the following non-local game:

1. Charlie sends two uniformly random generated bits x and y to Alice and Bob respectively.
2. Alice and Bob will announce their individual bits a and b to Charlie.
3. Alice and Bob win the game if and only if $x \,\&\, y = a \oplus b$.

The following truth table is obtained for $x \,\&\, y$:

x	y	$x \,\&\, y$
0	0	0
0	1	0
1	0	0
1	1	1

Since the game is non-local, Alice and Bob cannot communicate. Then, observe that the announced bits a and b are simply functions that can be defined as $a = f_{SC}(x)$ and $b = g_{SC}(y)$, where f_{SC} and g_{SC} are a map based on a shared classical strategy SC between Alice and Bob made prior to the starting of the game to help them determine which are the outputs that would give them the highest chance to win the game. Alice and Bob can easily determine that the strategy would be to simply always output $a = b = 0$ which gives them $p_{\text{win}} = \frac{3}{4} = 75\%$.

6.2.2 Quantum

Suppose that Alice and Bob are allowed to use a quantum strategy SQ, which involves choosing their optimal measurement bases prior to the start of the game. The game is now:

1. Alice shares $|\Phi^+\rangle_{AB}$ with Bob.
2. Charlie sends two uniformly random generated bits x and y to Alice and Bob respectively.
3. Alice measures ρ_A in the basis $x == 0\ ?\ \{|0\rangle, |1\rangle\} : \{|+\rangle, |-\rangle\}$.
4. Bob measures ρ_B in the basis $y == 0\ ?\ \{u_0, u_1\} = \{\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, -\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\}$ $: \{v_0, v_1\} = \{\cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle, \sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle\}$
5. Alice and Bob will announce their measurement outcomes a and b to Charlie.
6. Alice and Bob win the game if and only if $x \,\&\, y = a \oplus b$.

Consider the case where $x = y = 0$. Then, we have: $p_{\text{win}} = \text{tr}(|\Phi^+\rangle\langle\Phi^+|0u_0\rangle\langle 0u_0|) + \text{tr}(|\Phi^+\rangle\langle\Phi^+|1u_1\rangle\langle 1u_1|)$ $= |\langle 0u_0|\Phi^+\rangle|^2 + |\langle 1u_1|\Phi^+\rangle|^2 = |\frac{\cos\frac{\pi}{8}}{\sqrt{2}}|^2 + |-\frac{\cos\frac{\pi}{8}}{\sqrt{2}}|^2 = \cos^2\frac{\pi}{8} \approx 85\%$.

Similar computations can be made for the other three permutations of x and y. The same evaluations do not extend to a third party in a tripartite version of the game due to monogamy of entanglement, i.e. if $|\psi\rangle_{ABE} = |\Phi^+\rangle_{AB} \otimes |\theta\rangle_E$, then Eve has no correlation with Alice or Bob and therefore $p_{guess_E} = \frac{1}{2}$.

6.2.3 Tsirelson's bound

Tsirelson's bound demonstrates that the quantum strategy SQ used is optimal. The probability of winning the CHSH game can be expressed as a sum of the winning quadruples $(a, b|x, y)$ averaged over the four possible pairs (x, y) in the form:

$$p_{\text{win}} = \frac{1}{4} \sum_{a \oplus b = x \& y} p_{a,b|x,y} = \frac{1}{4}(p_{0,0|0,0} + p_{0,0|0,1} + p_{0,0|1,0} + p_{0,1|1,1} + p_{1,0|1,1} + p_{1,1|0,0} + p_{1,1|0,1} + p_{1,1|1,0})$$

Let $|\psi\rangle_{AB} \in H_A \otimes H_B$ be an arbitrary entangled bipartite state shared by Alice and Bob over their respective Hilbert spaces. Upon receiving x and y, Alice and Bob make their respective measurements. Let these measurements be the POVMs $\{A_x^a\}$ and $\{B_y^b\}$ for $a, b \in \{0, 1\}$. Alice and Bob will eventually announce their measurement outcomes a and b. Then, $p_{a,b|x,y} = \text{tr}((A_x^a \otimes B_y^b)|\psi\rangle\langle\psi|) = \langle\psi|_{AB}(A_x^a \otimes B_y^b)|\psi\rangle_{AB}$ using the Born rule.

For $x, y \in \{0, 1\}$, define $|i_x\rangle = (A_x \otimes \mathbb{I}_B)|\psi\rangle_{AB}$ and $|j_y\rangle = (\mathbb{I}_A \otimes B_y)|\psi\rangle_{AB}$. Then, we have:

$\langle i_x|j_y\rangle = \langle\psi|_{AB}(A_x \otimes \mathbb{I}_B)(\mathbb{I}_A \otimes B_y)|\psi\rangle_{AB} = \langle\psi|_{AB}(A_x \otimes B_y)|\psi\rangle_{AB}$
$= \langle\psi|_{AB}(A_x^0 \otimes B_y^0)|\psi\rangle_{AB} - \langle\psi|_{AB}(A_x^0 \otimes B_y^1)|\psi\rangle_{AB} - \langle\psi|_{AB}(A_x^1 \otimes B_y^0)|\psi\rangle_{AB} + \langle\psi|_{AB}(A_x^1 \otimes B_y^1)|\psi\rangle_{AB}$
$= p_{0,0|x,y} - p_{0,1|x,y} - p_{1,0|x,y} + p_{1,1|x,y}$

This leads to the following:

$$\langle i_x|j_y\rangle = \begin{cases} p_{0,0|x,y} + p_{0,1|x,y} + p_{1,0|x,y} + p_{1,1|x,y} - 2p_{0,1|x,y} - 2p_{1,0|x,y} = 1 - 2p_{0,1|x,y} - 2p_{1,0|x,y} & \text{for } (x, y) = (1, 1) \\ 2p_{0,0|x,y} + 2p_{1,1|x,y} - p_{0,0|x,y} - p_{0,1|x,y} - p_{1,0|x,y} - p_{1,1|x,y} = 2p_{0,0|x,y} + 2p_{1,1|x,y} - 1 & \text{for } (x, y) \neq (1, 1) \end{cases}$$

This gives us $p_{0,1|x,y} + p_{1,0|x,y} = \frac{1}{2} - \frac{\langle i_x|j_y\rangle}{2}$ and $p_{0,0|x,y} + p_{1,1|x,y} = \frac{1}{2} + \frac{\langle i_x|j_y\rangle}{2}$.

Simplifying, $p_{\text{win}} = \frac{1}{4}(\frac{1}{2} - \frac{\langle i_1|j_1\rangle}{2} + \frac{1}{2} + \frac{\langle i_0|j_0\rangle}{2} + \frac{1}{2} + \frac{\langle i_0|j_1\rangle}{2} + \frac{1}{2} + \frac{\langle i_1|j_1\rangle}{2}) = \frac{1}{2} + \frac{1}{8}(\langle i_0|j_0\rangle + \langle i_0|j_1\rangle + \langle i_1|j_0\rangle - \langle i_1|j_1\rangle)$.

Since $\{A_x^a\}$ and $\{B_y^b\}$ are POVMs, they have $\lambda \in [-1, 1]$. Then, $|||i_x\rangle||^2, |||j_y\rangle||^2 \leq |||\psi\rangle_{AB}||^2 = 1$.

Finally, we have:

$$\langle i_0|j_0\rangle + \langle i_0|j_1\rangle + \langle i_1|j_0\rangle - \langle i_1|j_1\rangle \leq \frac{1}{\sqrt{2}}(|||i_0\rangle||^2 + |||i_1\rangle||^2 + |||j_0\rangle||^2 + |||j_1\rangle||^2) \leq 2\sqrt{2}$$

$$p_{\text{win}} = \frac{1}{2} + \frac{2\sqrt{2}}{8} = \cos^2\frac{\pi}{8}$$

7 Quantum key distribution

Recall the two requirements of secure key distribution in cryptography:

For a defined error bound ϵ,

1. ϵ_c-correctness: The probability that Alice and Bob do not abort and their keys $k_A \neq k_B$ must not exceed ϵ_c, given by $\Pr(k_a \ \& \ k_b \ \& \ k_a \neq k_b) \leq \epsilon_c$.
2. ϵ_s-secrecy: The probability that Alice and Bob do not abort depends on the difference between the actual state $\rho_{kE}^{\text{actual}}$, which is the joint state of Alice's key k_A and Eve, and ideal state $\rho_{kE}^{\text{ideal}} = \frac{I_k}{2} \otimes \rho_E$, where Eve has no correlation with Alice's key, given by $(1 - \Pr(\text{Abort}))||\rho_{kE}^{\text{actual}} - \rho_{kE}^{\text{ideal}}|| \leq \epsilon_s$.

These are the goals to be met by QKDs.

7.1 Assumptions

1. All parties are bound by the laws of quantum physics.
2. Alice and Bob behave honestly.
3. Alice and Bob have access to private workstations that Eve has no access to.
4. Computations performed by Alice and Bob are done perfectly, including uniform random number generation.
5. Alice and Bob have access to a classical authenticated channel, i.e. a non-secret channel that Alice and Bob send classical bits through, and Eve can eavesdrop on but she cannot impersonate Alice or Bob, and a quantum communication channel, i.e. a non-secret channel that Alice and Bob send qubits through, and Eve can eavesdrop on.

Therefore, if Alice prioritises the message authenticity, she should always use the classical authenticated channel.

7.2 Prepare-and-measure BB84

The BB84 protocol is the following:

1. Alice uniformly random generates two bits $x, \theta \in \{0, 1\}$ and prepares a state $H^\theta|x\rangle$ that is sent to Bob.
2. Bob uniformly generates one bit $\theta' \in \{0, 1\}$ and measures $H^\theta|x\rangle$ using θ'.
3. The post-measurement state is given by $\rho_{XB}^{\theta'} = \sum_{x\in\{0,1\}} |x\rangle\langle x|_{X_A} \otimes H^{\theta'}|x\rangle\langle x|_B H^{\theta'}$.

   This produces the following: $\begin{cases} \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) & \text{for } \theta' = 0 \\ \frac{1}{2}(|0+\rangle\langle 0+| + |1-\rangle\langle 1-|) & \text{for } \theta' = 1 \end{cases}$
4. Bob informs Alice that he has received and measured $H^\theta|x\rangle$.
5. Alice and Bob announce θ and θ' respectively.
6. Alice and Bob discard the measurement if $\theta = \theta'$.
7. Repeat the above process for a desired key length.
8. Alice and Bob perform parameter estimation to check whether their outcomes x_i and y_i in the ith round are perfectly correlated. This is done by testing a predetermined subset of all the rounds they played. This subset is small so that Eve cannot get much information, but large enough for testing purposes.

9. Alice announces her measured results $x_i \; \forall \; i \in$ subset and Bob checks them against his measured results $y_i \; \forall \; i \in$ subset. If $|\{i : x_i \neq y_i\}| > \epsilon \rightarrow$ if you lose enough rounds, it's not just noise interference and it can be deduced that Eve is present, so abort the protocol.
10. Alice and Bob perform information reconciliation.
11. Alice and Bob perform privacy amplification, further reducing Eve's knowledge about their current state.
12. Alice and Bob produce their final raw keys k_A and k_B, with a high probability that $k_A = k_B$.

7.3 Entanglement-based BBM92

The BBM92 protocol is the following:

1. Alice shares $|\Phi^+\rangle_{AB}$ with Bob.
2. Alice uniformly generates one bit $\theta \in \{0, 1\}$ and measures ρ_A using $\{H^\theta|0\rangle, H^\theta|1\rangle\}$.

   To obtain the same post-measurement state as BB84, Alice records her measurement as $\{|0\rangle, |1\rangle\}$ for either value of $\theta = 0, 1$, i.e. no change if $\theta = 0$ given computational basis measurements, but records $|+\rangle$ and $|-\rangle$ as $|0\rangle$ and $|1\rangle$ respectively if $\theta = 1$ given Hadamard basis measurements.
3. Bob uniformly generates one bit $\theta' \in \{0, 1\}$ and measures ρ_B using θ'.
4. Alice and Bob inform each other that they have performed their measurements.
5. Alice and Bob announce θ and θ' respectively.
6. Alice and Bob discard the measurement if $\theta = \theta'$.
7. Repeat the above process for a desired key length.
8. Alice and Bob perform parameter estimation to check whether their outcomes x_i and y_i in the ith round are perfectly correlated. This is done by testing a predetermined subset of all the rounds they played. This subset is small so that Eve cannot get much information, but large enough for testing purposes.
9. Alice announces her measured results $x_i \; \forall \; i \in$ subset and Bob checks them against his measured results $y_i \; \forall \; i \in$ subset. If $|\{i : x_i \neq y_i\}| > \epsilon \rightarrow$ if you lose enough rounds, it's not just noise interference and it can be deduced that Eve is present, so abort the protocol.
10. Alice and Bob perform information reconciliation.
11. Alice and Bob perform privacy amplification, further reducing Eve's knowledge about their current state.
12. Alice and Bob produce their final raw keys k_A and k_B, with a high probability that $k_A = k_B$.

Ideally, the state that Alice shares with Bob is maximally entangled. Then, by monogamy of entanglement, $\rho_{ABE} = \rho_{AB} \otimes \rho_E \Rightarrow$ Eve has no correlation with Alice or Bob and therefore $p_{guess_E} = \frac{1}{2}$.